

On Euclidean and Hermitian Self-Dual Cyclic Codes over \mathbb{F}_{2^r}

Odessa D. Consorte*

*Institute of Mathematics
University of the Philippines, Diliman, Quezon City, Philippines*

Lilibeth D. Valdez†

*Institute of Mathematics
University of the Philippines, Diliman, Quezon City, Philippines*

Abstract

Cyclic and self-dual codes are important classes of codes in coding theory. Jia, Ling and Xing [5] as well as Kai and Zhu [7] proved that Euclidean self-dual cyclic codes of length n over \mathbb{F}_q exist if and only if n is even and $q = 2^r$, where r is any positive integer. For n and q even, there always exists an $[n, \frac{n}{2}]$ self-dual cyclic code with generator polynomial $x^{\frac{n}{2}} + 1$ called the *trivial self-dual cyclic code*. In this paper we prove the existence of nontrivial self-dual cyclic codes of length $n = 2^\nu \cdot \bar{n}$, where \bar{n} is odd, over \mathbb{F}_{2^r} in terms of the existence of a nontrivial splitting (Z, X_0, X_1) of $\mathbb{Z}_{\bar{n}}$ by μ_{-1} , where Z, X_0, X_1 are unions of 2^r -cyclotomic cosets mod \bar{n} . We also express the formula for the number of cyclic self-dual codes over \mathbb{F}_{2^r} for each n and r in terms of the number of 2^r -cyclotomic cosets in X_0 (or in X_1).

We also look at Hermitian self-dual cyclic codes and show properties which are analogous to those of Euclidean self-dual cyclic codes. That is, the existence of nontrivial Hermitian self-dual codes over $\mathbb{F}_{2^{2\ell}}$ based on the existence of a nontrivial splitting (Z, X_0, X_1) of $\mathbb{Z}_{\bar{n}}$ by μ_{-2^ℓ} , where Z, X_0, X_1 are unions of $2^{2\ell}$ -cyclotomic cosets mod \bar{n} . We also determine the lengths at which nontrivial Hermitian self-dual cyclic codes exist and the formula for the number of Hermitian self-dual cyclic codes for each n .

Keywords: Cyclic codes, self-dual codes, splittings

*Electronic address: ocosorte@math.upd.edu.ph

†Electronic address: ldicuangco@math.upd.edu.ph; Corresponding author

1 Introduction

Cyclic codes have been widely studied and have found numerous applications in storage and communication systems due to the ease in their encoding/decoding. Both finite fields and rings have been considered as “alphabets” in the construction of cyclic codes. In this study, we focus on cyclic codes over finite fields.

For a code \mathcal{C} of length n and dimension k , denoted as an $[n, k]$ code over a finite field \mathbb{F}_q (q a power of a prime), its dual code, \mathcal{C}^\perp is defined to be $\{\mathbf{x} \in \mathbb{F}_q^n | \mathbf{x} \cdot \mathbf{c} = 0 \text{ for all } \mathbf{c} \in \mathcal{C}\}$. \mathcal{C}^\perp is an $[n, n - k]$ code. A code is said to be Euclidean self-dual if and only if $\mathcal{C} = \mathcal{C}^\perp$.

One method of constructing self-dual codes from cyclic codes is by extending cyclic codes whose length n and the characteristic of the field \mathbb{F}_q are relatively prime. Smid [11] showed that if an extended cyclic code is self-dual, then this cyclic code is a duadic code with splitting given by μ_{-1} . Ocampo [8] has generalized this to group codes (of which cyclic codes are a subclass) and similarly showed that for a group code \mathcal{C} , an ideal in the group ring $\mathbb{F}_{q^2}[G^*]$, the extended group code $\tilde{\mathcal{C}}$ is Euclidean self-dual if and only if \mathcal{C} is a split group code for some splitting ($Z = \{0\}, X_0, X_1$) of G by μ_{-1} .

The other method for constructing self-dual cyclic codes considers cyclic codes of even length. In 1983, Sloane [10] noticed that extensive research have been done regarding self-dual codes but cyclic self-dual codes in particular have not received much attention. He showed that the number of distinct cyclic self-dual binary codes of length $2^a b$ (b odd) depends on the number of pairs of asymmetric cyclotomic cosets modulo b . Jia et al. [5] and Kai et al. [7] generalized this to cyclic codes over \mathbb{F}_q . They proved that self-dual cyclic codes of length n over \mathbb{F}_q exist if and only if q is power of 2 and n is even. In particular, n and q are not relatively prime. This condition gives rise to repeated-root cyclic codes.

Repeated-root cyclic codes were first studied by Castagnoli et al. [1] and van Lint [12]. van Lint focused on binary cyclic codes of length $2n$ (n odd) obtained by the $|u|u + v|$ construction. He showed that using this construction, an infinite sequence of optimal cyclic codes with distance 4 can be obtained. Furthermore, these codes require low complexity decoding methods. On the other hand, Castagnoli et al. derived a parity check matrix and gave a formula for the minimum distance of repeated-root cyclic codes. They were able to find several repeated-root binary cyclic codes that contain the maximum number of codewords among all known binary codes of the same length and minimum distance. However, they have also demonstrated that repeated root cyclic codes are not better than general cyclic codes of the same length. In spite of this, it is still worthwhile to study repeated-root cyclic codes under which self-dual cyclic codes of even length are classified.

This paper is organized as follows. In Section 2, we give the notations that will be used in this paper and review some basic concepts regarding cyclic codes. The reader is referred to Huffman and Pless [4] for a more detailed discussion of cyclic codes. In Section 3, we focus on Euclidean self-dual cyclic codes over \mathbb{F}_{2^r} .

We look at previous results and use q -cyclotomic cosets mod \bar{n} and splittings of $\mathbb{Z}_{\bar{n}}$ to determine the existence of nontrivial self-dual cyclic codes. We then obtain analogous statements in Section 4 for Hermitian self-dual cyclic codes over $\mathbb{F}_{2^{2\ell}}$.

2 Notations and Basic Concepts

A cyclic code \mathcal{C} is a linear code of length n over a field \mathbb{F}_q , where q is a power of a prime such that if $\mathbf{c} = c_0c_1 \cdots c_{n-1} \in \mathcal{C}$, then its right cyclic shift $\mathbf{c} = c_{n-1}c_0 \cdots c_{n-2}$ is also an element of \mathcal{C} . We consider the bijective correspondence between vectors $\mathbf{c} = c_0c_1 \cdots c_{n-1}$ in \mathbb{F}_q^n and polynomials $c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$ in $\mathbb{F}_q[x]$ of degree at most $n-1$. The codeword \mathbf{c} cyclically shifted one to the right can be represented by $x \cdot c(x) = c_{n-1} + c_0x + \cdots + c_{n-2}x^{n-1}$ where we have set $x^n = 1$. Hence, the study of cyclic codes is equivalent to the study of the residue class ring $\mathbb{F}_q[x]/(x^n - 1)$. The study of ideals in this residue class ring hinges on factoring $x^n - 1$. Following the result of Jia et al. (Theorem 1 of [5]), we shall consider cyclic codes of even length throughout this paper. That is, let $n = 2^\nu \cdot \bar{n}$, where \bar{n} is odd, and ν is a positive integer.

To obtain the irreducible factors of $x^n - 1$, we recall the concept of q -cyclotomic cosets. Let a be a non-negative integer, $0 \leq a < \bar{n}$, and $\gcd(q, \bar{n}) = 1$, the **q -cyclotomic coset of a modulo \bar{n}** is the set

$$C_a = \{a, aq, aq^2, \dots, aq^{r-1}\}$$

where each element is computed modulo \bar{n} , r is the smallest positive integer such that $aq^r \equiv a \pmod{\bar{n}}$, and a is usually taken as the smallest number in the set. Note that the distinct q -cyclotomic cosets mod \bar{n} partition the set $\{0, 1, \dots, \bar{n}-1\}$.

Suppose $t = \text{ord}_{\bar{n}}(q)$, i.e. t is the smallest positive integer such that $q^t \equiv 1 \pmod{\bar{n}}$. If α is a primitive \bar{n}^{th} root of unity in \mathbb{F}_{q^t} , then the **minimal polynomial** of α^a over \mathbb{F}_q , is $f_a(x) = \prod_{i \in C_a} (x - \alpha^i)$. For \bar{n} and q relatively prime, the factorization of $x^{\bar{n}} - 1$ into pairwise-irreducible polynomials over \mathbb{F}_q is given by

$$x^{\bar{n}} - 1 = \prod_{a \in I} f_a(x),$$

where I is the complete set of q -cyclotomic coset representatives modulo \bar{n} . Hence

$$x^n - 1 = [x^{\bar{n}} - 1]^{2^\nu} = \prod_{a \in I} f_a(x)^{2^\nu}$$

has \bar{n} distinct roots with multiplicity 2^ν in its splitting field.

An $[n, k]$ cyclic code can be described by its generator polynomial. The **generator polynomial** of a code is the unique monic polynomial of degree $n - k$ that is a divisor of $x^n - 1$ in $\mathbb{F}_q[x]$. It is a product of the minimal polynomials of α^a where a is any element of I (defined above) over \mathbb{F}_q .

Suppose \mathcal{C} is an $[n, k]$ cyclic code with generator polynomial $g(x)$. The polynomial

$$p(x) = \frac{x^n - 1}{g(x)} = \sum_{i=0}^k p_i x^i$$

is called the *parity-check polynomial* of \mathcal{C} . Consequently, the generator polynomial of \mathcal{C}^\perp is defined as

$$p^*(x) = p_0^{-1} x^k p(x^{-1}).$$

3 Self-Dual Cyclic Codes

Jia et al. [5] and Kai et al. [7] proved that there exists at least one self-dual cyclic code of length n over \mathbb{F}_q if and only if q is a power of 2 and n is even. This code is the $[n, \frac{n}{2}]$ trivial self-dual cyclic code and has generator polynomial $x^{\frac{n}{2}} + 1$. Our aim is to determine the conditions under which nontrivial self-dual cyclic codes exist.

Let $f(x)$ be a polynomial in $\mathbb{F}_q[x]$. The **reciprocal polynomial** of $f(x)$ is the polynomial

$$f^*(x) = f_0^{-1} \cdot x^{\deg f} \cdot f(x^{-1}) = f_0^{-1} (f_k + f_{k-1}x + \cdots + f_0x^k),$$

where f_0 is the constant term of the polynomial $f(x)$. $f(x)$ is called a **self-reciprocal** polynomial if $f(x) = f^*(x)$.

It is known that if $\alpha^a, \alpha^{qa}, \dots, \alpha^{q^{k-1}a}$ are the nonzero roots of f in some extension field of \mathbb{F}_q , then $\alpha^{-a}, \alpha^{-qa}, \dots, \alpha^{-q^{k-1}a}$ are the nonzero roots of f^* in that extension field. If $f(x)$ is irreducible over \mathbb{F}_q , so is $f^*(x)$. Hence, if $f_a(x) = \prod_{i \in C_a} (x - \alpha^i)$ is the minimal polynomial of α^a over \mathbb{F}_q , then its reciprocal polynomial is

$$f_a^*(x) = \prod_{i \in C_a} (x - \alpha^{-i}) = \prod_{i \in C_{-a}} (x - \alpha^i) = f_{-a}(x).$$

This implies that if C_a is the q -cyclotomic coset that corresponds to the minimal polynomial $f_a(x)$ then C_{-a} is the q -cyclotomic coset that corresponds to its reciprocal polynomial $f_a^*(x)$. Note that $C_{-a} = \mu_{-1}C_a$, where the **multiplier** μ_{-1} is defined by $i\mu_{-1} \equiv -i \pmod{\bar{n}}$ for each i in $\{0, 1, 2, \dots, \bar{n} - 1\}$.

For $n = 2^\nu \cdot \bar{n}$ and $q = 2^r$, where \bar{n}, q are relatively prime, $x^{\bar{n}} + 1$ can be written as a product of distinct irreducible polynomial factors as [5]

$$x^{\bar{n}} + 1 = f_1(x) \cdots f_s(x) h_1(x) h_1^*(x) \cdots h_t(x) h_t^*(x),$$

where the $f_i(x)$'s are monic, irreducible, self-reciprocal polynomials over \mathbb{F}_{2^r} and $h_j(x), h_j^*(x)$ form a pair of reciprocal polynomials which are also monic and irreducible over \mathbb{F}_{2^r} . Hence,

$$x^n + 1 = (x^{\bar{n}} + 1)^{2^\nu} = f_1(x)^{2^\nu} \cdots f_s(x)^{2^\nu} h_1(x)^{2^\nu} h_1^*(x)^{2^\nu} \cdots h_t(x)^{2^\nu} h_t^*(x)^{2^\nu}.$$

Theorem 2 of [5] states that if $x^n + 1$ is factorized as above, a cyclic code of length n is self-dual over \mathbb{F}_{2^r} if and only if its generator polynomial is of the form

$$g(x) = f_1(x)^{2^{\nu-1}} \cdots f_s(x)^{2^{\nu-1}} h_1(x)^{\beta_1} h_1^*(x)^{2^\nu - \beta_1} \cdots h_t(x)^{\beta_t} h_t^*(x)^{2^\nu - \beta_t}$$

where $0 \leq \beta_i \leq 2^\nu$ for each $1 \leq i \leq t$.

Note that using this factorization, the generator polynomial of the trivial self-dual cyclic code can be written as

$$x^{\frac{n}{2}} + 1 = f_1(x)^{2^{\nu-1}} \cdots f_s(x)^{2^{\nu-1}} h_1(x)^{2^{\nu-1}} h_1^*(x)^{2^{\nu-1}} \cdots h_t(x)^{2^{\nu-1}} h_t^*(x)^{2^{\nu-1}}.$$

It was earlier noted that the $f_i(x)$'s, $h_j(x)$'s, $h_j^*(x)$'s are minimal polynomials that correspond to some q -cyclotomic coset C_i , C_j , and C_{-j} respectively. Thus, aside from studying the factors of $x^n - 1$, we can look at the 2^r -cyclotomic cosets mod \bar{n} in the characterization of self-dual cyclic codes.

Definition 3.1 [3] Let $\gcd(q, \bar{n}) = 1$. A **splitting** of $\mathbb{Z}_{\bar{n}}$ by the multiplier $\mu_b, b \neq 0$ is a triple (Z, X_0, X_1) which satisfies the following conditions:

1. Z, X_0, X_1 are unions of q -cyclotomic cosets mod \bar{n} such that $\mathbb{Z}_{\bar{n}} = Z \cup X_0 \cup X_1$ and $Z \cap X_0 \cap X_1 = \emptyset$.
2. $\mu_b(Z) = Z, \mu_b(X_0) = X_1$ and $\mu_b(X_1) = X_0$.

We say that a splitting is trivial if X_0 and X_1 are both empty.

Proposition 3.2 Let $\gcd(q, \bar{n}) = 1$. In the factorization of $x^{\bar{n}} - 1$ over \mathbb{F}_q , there exists at least one pair of reciprocal, monic, irreducible polynomials if and only if there exists a nontrivial splitting (Z, X_0, X_1) of $\mathbb{Z}_{\bar{n}}$ by μ_{-1} and each q -cyclotomic coset in Z is fixed set-wise by μ_{-1} .

Proof Suppose that over \mathbb{F}_q , $x^{\bar{n}} - 1$ factors into $f_1(x) \cdots f_s(x) h_1(x) h_1^*(x) \cdots h_\ell(x) h_\ell^*(x)$, where $\ell \geq 1$, the $f_k(x)$'s are monic, irreducible, and self-reciprocal, while $h_j(x)$ and $h_j^*(x)$ for $1 \leq j \leq \ell$ comprise a pair of reciprocal polynomials which are monic and irreducible. Let C_1, \dots, C_s be the q -cyclotomic cosets which correspond to the minimal polynomials $f_1(x), \dots, f_s(x)$ respectively. Since the $f_i(x)$'s are self-reciprocal, $\mu_{-1}C_k = C_k$ for all $k = 1, \dots, s$. Take $Z = C_1 \cup \cdots \cup C_s$.

On the other hand, $h_j^*(x)$ is the reciprocal polynomial of $h_j(x)$, where $h_j^*(x) \neq h_j(x)$. Hence, $h_j^*(x) = h_{-j}(x)$ and $\mu_{-1}C_j = C_{-j}$, $j \neq -j$. Take $X_0 = \cup_j C_j$ and $X_1 = \cup_j C_{-j}$. Since $j \geq 1$, we obtain a nontrivial splitting (Z, X_0, X_1) of $\mathbb{Z}_{\bar{n}}$ by μ_{-1} .

Conversely, suppose there exists a nontrivial splitting of $\mathbb{Z}_{\bar{n}}$ by μ_{-1} . That is,

$$\{0, 1, \dots, \bar{n} - 1\} = Z \cup X_0 \cup X_1 \text{ s.t. } Z \cap X_0 \cap X_1 = \emptyset$$

and

$$X_0, X_1 \neq \emptyset, \mu_{-1}X_0 = X_1, \mu_{-1}X_1 = X_0$$

where Z, X_0, X_1 are unions of q -cyclotomic cosets modulo \bar{n} , and each q cyclotomic coset in Z is fixed set wise by μ_{-1} . Let $Z = C_{z_1} \cup \dots \cup C_{z_k}$ for some $k \geq 1$. Since $\mu_{-1}C_{z_i} = C_{z_i}$ for $i = 1, \dots, k$, the corresponding minimal polynomials $f_0(x), f_{z_1}(x), \dots, f_{z_k}(x)$ are self-reciprocal.

Since X_0 and X_1 are both non-empty, there exists at least one q -cyclotomic coset in X_0 and X_1 . Suppose $X_0 = \cup_j C_j$ for $j \geq 1$. Then $\mu_{-1}X_0 = X_1$ implies $X_1 = \cup_j C_{-j}$. For $j \geq 1$, let $h_j(x)$ be the minimal polynomial which corresponds to C_j and $h_{-j}(x)$ to C_{-j} . But, $h_{-j}(x) = h_j^*(x)$ for each j . Hence, $h_j(x)$ and $h_{-j}(x)$ form a pair of reciprocal polynomials in the factorization of $x^{\bar{n}} - 1$. \square

This proposition and the factorization condition given by Jia et al. (Theorem 2 of [5]) lead to the following statement.

Theorem 3.3 *A nontrivial Euclidean self-dual cyclic code \mathcal{C} of length $n = 2^\nu \cdot \bar{n}$ over \mathbb{F}_{2^r} exists if and only if there exists a nontrivial splitting (Z, X_0, X_1) of $\mathbb{Z}_{\bar{n}}$ by μ_{-1} where each q -cyclotomic coset in Z is fixed set-wise by μ_{-1} .*

We can then restate Corollary 1 of [5] using q -cyclotomic cosets modulo \bar{n} and the splitting (Z, X_0, X_1) as follows. (Note that this is similar to Theorem 5 of [9]).

Corollary 3.4 *For $n = 2^\nu \cdot \bar{n}, r > 0$, the number of $[n, \frac{n}{2}]$ self-dual cyclic codes over \mathbb{F}_{2^r} is exactly*

$$(2^\nu + 1)^t$$

where t is the number of 2^r -cyclotomic cosets in X_0 (or in X_1).

Next, we want to determine the lengths n for which nontrivial self-dual cyclic codes over \mathbb{F}_{2^r} exist. Kai et al. [7] has proved a similar theorem. We will present an alternate proof using the splittings of $\mathbb{Z}_{\bar{n}}$ by μ_{-1} described earlier. We first state the following lemma.

Lemma 3.5 *For \bar{n} odd, let $\mathbb{Z}_{\bar{n}}$ be partitioned into C_0, \dots, C_ℓ where each C_i is a q -cyclotomic coset modulo \bar{n} . Then, for all $a \neq -a$ in $\{1, \dots, \ell\}$, $C_a = C_{-a}$ if and only if $q^k \equiv -1 \pmod{\bar{n}}$ for any positive integer k .*

Proof Suppose $a \neq -a$ and $C_a = C_{-a}$. Then, $\{a, qa, q^2a, \dots, q^{m-1}a\} = \{-a, q(-a), q^2(-a), \dots, q^{m-1}(-a)\}$. This implies that there exists k , $1 \leq k \leq m-1$ such that $a \equiv q^k(-a) \pmod{\bar{n}}$. Hence, $q^k \equiv -1 \pmod{\left(\frac{\bar{n}}{\gcd(a, \bar{n})}\right)}$. Taking $a = 1$, we have $C_1 = C_{-1}$ if and only if $q^k \equiv -1 \pmod{\bar{n}}$. Then $C_j = C_{-j}$ for $j = 1, \dots, \ell$ since $q^k \equiv -1 \pmod{\bar{n}}$ implies $jq^k \equiv -j \pmod{\bar{n}}$. Conversely, if $q^k \equiv -1 \pmod{\bar{n}}$ then $aq^k \equiv -a \pmod{\bar{n}}$. Hence $C_a = C_{-a}$ for all $a = 1, \dots, \ell$. \square

Theorem 3.6 *Nontrivial Euclidean self-dual cyclic codes of length $n = 2^\nu \cdot \bar{n}$ ($\nu \in \mathbb{Z}^+, \bar{n}$ odd) over \mathbb{F}_{2^r} , $r \in \mathbb{Z}^+$ exist if and only if $2^{rk} \not\equiv -1 \pmod{\bar{n}}$ for all positive integers k .*

Proof Suppose \mathcal{C} is a nontrivial Euclidean self-dual cyclic code of length n over \mathbb{F}_{2^r} . By Theorem 3.3, there exists a nontrivial splitting (Z, X_0, X_1) of $\mathbb{Z}_{\bar{n}}$ by μ_{-1} and so $X_0 = \cup_j C_j$, for $j \geq 1$. By Definition 3.1, $\mu_{-1}(X_0) = \mu_{-1}(\cup_j C_j) = \cup_j C_{-j} = X_1$ where $X_0 \cap X_1 = \emptyset$. Then, $C_j \neq C_{-j}$ for at least one j . Using Lemma 3.5, we conclude that $2^{rk} \not\equiv -1 \pmod{n}$ for all $k \in \mathbb{Z}^+$. The converse is proved similarly. \square

4 Hermitian Self-Dual Cyclic Codes

We now consider cyclic codes over \mathbb{F}_{q^2} , where q is a power of a prime p . Let $\mathbf{x} = (x_0, x_1, \dots, x_{n-1})$ and $\mathbf{y} = (y_0, y_1, \dots, y_{n-1})$ be vectors in $\mathbb{F}_{q^2}^n$. Consider the involution $\bar{\cdot} : a \mapsto a^q$ defined on \mathbb{F}_{q^2} . The *Hermitian scalar product* of \mathbf{x} and \mathbf{y} is defined to be $\mathbf{x} \cdot \bar{\mathbf{y}} = \sum_{i=0}^{n-1} x_i \bar{y}_i = \sum_{i=0}^{n-1} x_i y_i^q$.

Let \mathcal{C} be an $[n, k]$ cyclic code over \mathbb{F}_{q^2} . The **Hermitian dual** of \mathcal{C} is the set $\mathcal{C}^{\perp_H} = \{\mathbf{u} \in \mathbb{F}_{q^2}^n \mid \mathbf{u} \cdot \bar{\mathbf{w}} = 0 \text{ for all } \mathbf{w} \in \mathcal{C}\}$. We say that a code \mathcal{C} is **Hermitian self-dual** if $\mathcal{C} = \mathcal{C}^{\perp_H}$.

We extend the involution map to polynomials in $\mathbb{F}_{q^2}[x]$. For $f(x) = f_0 + f_1x + \dots + f_{n-1}x^{n-1}$ in $\mathbb{F}_{q^2}[x]$, we set $\overline{f(x)} = \overline{f_0} + \overline{f_1}x + \dots + \overline{f_{n-1}}x^{n-1}$. Let $f(x)$ be a polynomial in $\mathbb{F}_{q^2}[x]$ and $f^*(x)$ its reciprocal polynomial as defined earlier. The *conjugate reciprocal polynomial* of $f(x)$ is denoted as $f^\dagger(x)$ and is equal to $\overline{f^*(x)}$. $f(x)$ is said to be *self-conjugate reciprocal* if $f(x) = f^\dagger(x)$. Otherwise, $f(x)$ and $f^\dagger(x)$ form a conjugate-reciprocal pair.

Let \mathcal{C} be a nonzero $[n, k]$ cyclic code over \mathbb{F}_{q^2} generated by $g(x)$. If $p(x)$ is the parity-check polynomial of \mathcal{C} , then the generator polynomial of \mathcal{C}^{\perp_H} is $p^\dagger(x)$. Hence \mathcal{C} is Hermitian self-dual if and only if $g(x) = p^\dagger(x)$.

Jitman et al. [6] have shown that Hermitian self-dual abelian codes in $\mathbb{F}_{q^2}[G]$ ($\text{char } \mathbb{F}_{q^2} = p$; order of the finite abelian group $G = mp^k$, $p \nmid m$) exist if and only if $p = 2$ and $k \geq 1$. We only consider the cyclic case i.e., Hermitian self-dual cyclic codes over \mathbb{F}_{q^2} exist if and only if $q = 2^{2\ell}$ and n is even. A Hermitian self-dual cyclic code over this field of length n and dimension $n/2$ can always be constructed. Let $x^n - 1 = x^n + 1 = (x^{n/2} + 1)^2$. Take $g(x) = x^{n/2} + 1$. The parity check polynomial, $p(x) = x^{n/2} + 1 = p^*(x) = p^\dagger(x)$. Hence, the code generated by $g(x) = x^{n/2} + 1$ is not only Euclidean self-dual but also Hermitian self-dual. It will also be referred to as the trivial Hermitian self-dual cyclic code.

Consequently, in this section, we will consider codes of even length, $n = 2^\nu \cdot \bar{n}$ over $\mathbb{F}_{2^{2\ell}}$ and characterize nontrivial Hermitian self-dual cyclic codes over this field. Note that Dicuangco et al.[2] have proven that for a cyclic code \mathcal{C} over \mathbb{F}_{q^2} of odd length, the extended code is Hermitian self-dual if and only if \mathcal{C} is an odd-like duadic code split by μ_{-q} . We use Theorem 3.9 in [6] as a lemma to

prove the existence of nontrivial Hermitian self-dual cyclic of length n over $\mathbb{F}_{2^{2\ell}}$ using splittings of $\mathbb{Z}_{\overline{n}}$.

Lemma 4.1 (Theorem 3.9, [6]) *Let $n = 2^\nu \cdot \overline{n}$ where ν is a positive integer and \overline{n} is odd. Over $\mathbb{F}_{2^{2\ell}}[x]$, let $x^n + 1$ be factored as*

$$x^n + 1 = [x^{\overline{n}} + 1]^{2^\nu} = \left[f_1(x) \dots f_s(x) h_1(x) h_1^\dagger(x) \dots h_t(x) h_t^\dagger(x) \right]^{2^\nu}$$

where the f_i 's are monic, irreducible, self-conjugate reciprocal polynomials and h_j, h_j^* which are also monic and irreducible form a conjugate-reciprocal pair for $1 \leq j \leq t$. A cyclic code \mathcal{C} of length n is Hermitian self-dual over $\mathbb{F}_{2^{2\ell}}$ if and only if its generator polynomial is of the form

$$g(x) = f_1^{2^{\nu-1}}(x) \dots f_s(x)^{2^{\nu-1}} h_1(x)^{\gamma_1} h_1^\dagger(x)^{2^\nu - \gamma_1} \dots h_t^{\gamma_t}(x) h_t^\dagger(x)^{2^\nu - \gamma_t}$$

where $0 \leq \gamma_i \leq 2^\nu$ for each i .

We now discuss the relationship between $2^{2\ell}$ -cyclotomic cosets and conjugate-reciprocal polynomials. For a polynomial $f_a(x)$ in $\mathbb{F}_{2^{2\ell}}[x]$ where $f_a(x) = \prod_{i \in C_a} (x - \alpha^i)$ and $C_a = \{a, 2^{2\ell}a, \dots, 2^{2\ell r}a\}$ is the $2^{2\ell}$ -cyclotomic coset containing a , the nonzero roots of $f_a(x)$ in some extension field of $\mathbb{F}_{2^{2\ell}}$ are $\alpha^a, \dots, \alpha^{2^{2\ell r}a}$. Using the definition of the conjugate-reciprocal polynomial and involution in $\mathbb{F}_{2^{2\ell}}[x]$, we can write

$$f_a^\dagger(x) = f_0^{-2^\ell} x^k \prod_{i \in C_a} (x^{-1} - \alpha^{2^\ell i}) = \prod_{i \in C_a} (x - \alpha^{-2^\ell i}) = \prod_{i \in C_{(-2^\ell a)}} (x - \alpha^i).$$

Hence, if the $2^{2\ell}$ -cyclotomic coset C_a corresponds to the minimal polynomial $f_a(x)$ in $\mathbb{F}_{2^{2\ell}}$, then $C_{(-2^\ell a)} = \mu_{(-2^\ell)} C_a$ corresponds to the conjugate-reciprocal polynomial of $f_a(x)$ which is $f_a^\dagger(x)$.

We can use this property to prove the following proposition in a manner similar to the proof of Proposition 3.2 but instead of reciprocal polynomials, we use conjugate-reciprocal polynomials and instead of a splitting by μ_{-1} , we consider the splitting by μ_{-2^ℓ} .

Proposition 4.2 *In the factorization of $x^{\overline{n}} - 1$ over $\mathbb{F}_{2^{2\ell}}$, there exists at least one pair of conjugate-reciprocal, monic, irreducible polynomials if and only if there exists a nontrivial splitting (Z, X_0, X_1) of $\mathbb{Z}_{\overline{n}}$ by μ_{-2^ℓ} and each $2^{2\ell}$ -cyclotomic coset in Z is fixed set-wise by μ_{-2^ℓ} .*

The following theorem which is analogous to Theorem 3.3 can be shown to be true by using Proposition 4.2 instead of Proposition 3.2 in the proof.

Theorem 4.3 *A nontrivial Hermitian self-dual cyclic code \mathcal{C} of length $n = 2^\nu \cdot \overline{n}$ ($\nu \in \mathbb{Z}^+, \overline{n}$ odd) over $\mathbb{F}_{2^{2\ell}}$ exists if and only if there exists a nontrivial splitting (Z, X_0, X_1) of $\mathbb{Z}_{\overline{n}}$ by μ_{-2^ℓ} and each $2^{2\ell}$ -cyclotomic coset in Z is fixed setwise by μ_{-2^ℓ} .*

A corollary to this gives the number of Hermitian self-dual cyclic codes over $\mathbb{F}_{2^{2\ell}}$.

Corollary 4.4 *For $n = 2^\nu \cdot \bar{n}$, the number of $[n, \frac{n}{2}]$ Hermitian self-dual cyclic codes over $\mathbb{F}_{2^{2\ell}}$ is exactly*

$$(2^\nu + 1)^t$$

where t is the number of $2^{2\ell}$ -cyclotomic cosets in X_0 (or in X_1).

We can also determine the lengths n for which nontrivial Hermitian self-dual cyclic codes over $\mathbb{F}_{2^{2\ell}}$ exist as follows.

Lemma 4.5 *For $q = 2^\ell$ and \bar{n} odd, let $\mathbb{Z}_{\bar{n}}$ be partitioned into C_0, \dots, C_j where each C_i is a q^2 -cyclotomic coset modulo \bar{n} . Then, for all $a \neq -a$ in $\{1, \dots, j\}$, $C_a = C_{-qa}$ if and only if $q^{2k+1} \equiv -1 \pmod{\bar{n}}$ for any positive integer k .*

Proof Let C_0, \dots, C_j be the q^2 -cyclotomic cosets mod \bar{n} . Suppose $C_a = C_{-qa}$. Then, $\{a, q^2a, \dots, q^{2(m-1)} \cdot a\} = \{-qa, -q^3a, \dots, -q \cdot q^{2(m-1)} \cdot a\}$. This implies that there exists $k \in \mathbb{Z}$ where $1 \leq k \leq m-1$ such that $a \equiv q^{2k} \cdot -qa \pmod{\bar{n}}$. That is, $q^{2k+1} \equiv -1 \pmod{\left(\frac{\bar{n}}{\gcd(a, \bar{n})}\right)}$. If $a = 1$, $C_1 = C_{-1}$ if and only if $q^{2k+1} \equiv -1 \pmod{\bar{n}}$. Then $C_i = C_{-qi}$ for $i = 1, \dots, j$ since $q^{2k+1} \equiv -1 \pmod{\bar{n}}$ implies $iq^{2k+1} \equiv -i \pmod{\bar{n}}$. Conversely, if $q^{2k+1} \equiv -1 \pmod{\bar{n}}$ then $aq^{2k+1} \equiv -a \pmod{\bar{n}}$. Hence $C_a = C_{-qa}$ for all $a = 1, \dots, j$. \square

Using this lemma instead of Lemma 3.5 in the proof of Theorem 3.6, we can show that the following theorem holds.

Theorem 4.6 *Nontrivial Hermitian self-dual cyclic codes of length $n = 2^\nu \cdot \bar{n}$ ($\nu \in \mathbb{Z}^+$, \bar{n} odd) over $\mathbb{F}_{2^{2\ell}}$ exist if and only if $2^{\ell(2k+1)} \not\equiv -1 \pmod{\bar{n}}$ for all positive integers k .*

Table 1 shows the values of n for which nontrivial Hermitian self-dual cyclic codes over \mathbb{F}_4 exist and the number of Hermitian self-dual codes (including the trivial Hermitian self-dual code) for each n computed using Corollary 4.4. Here, $n = 2^\nu \cdot \bar{n}$ where \bar{n} is odd and t = number of 4-cyclotomic cosets in X_0 (or X_1). The highest minimum distance (HMinD) of the cyclic code of length n for $n \leq 100$ was computed using MAGMA.

Acknowledgment

The authors gratefully acknowledge financial support from the National Research Council of the Philippines.

Table 1: Number of Hermitian Self-Dual Cyclic Codes over \mathbb{F}_4

n	\bar{n}	ν	t	No. of HSD	HMinD	n	\bar{n}	ν	t	No. of HSD
10	5	1	1	3	4	158	79	1	1	3
14	7	1	1	3	4	160	5	5	1	33
20	5	2	1	5	4	164	41	2	2	25
26	13	1	1	3	6	168	21	3	3	729
28	7	2	1	5	4	170	85	1	11	177147
30	15	1	3	27	8	174	87	1	3	27
34	17	1	2	9	8	178	89	1	4	81
40	5	3	1	9	6	180	45	2	5	3125
42	21	1	3	27	8	182	91	1	8	6561
46	23	1	1	3	8	184	23	3	1	9
50	25	1	2	9	4	186	93	1	9	19683
52	13	2	1	5	6	188	47	2	1	5
56	7	3	1	9	6	190	95	1	3	27
58	29	1	1	3	12	194	97	1	2	9
60	15	2	3	125	8	196	49	2	2	25
62	31	1	3	27	10	200	25	3	2	81
68	17	2	2	25	12	202	101	1	1	3
70	35	1	4	81	14	204	51	2	6	15625
74	37	1	1	3	12	206	103	1	1	3
78	39	1	3	27	12	208	13	4	1	17
80	5	4	1	17	6	210	105	1	12	531441
82	41	1	2	9	12	212	53	2	1	5
84	21	2	3	125	10	218	109	1	3	27
90	45	1	5	243	8	220	55	2	3	125
92	23	2	1	5	8	222	111	1	3	27
94	47	1	1	3	12	224	7	5	1	33
98	49	1	2	9	4	226	113	1	4	81
100	25	2	2	25	8	228	57	2	2	25
102	51	1	6	729		230	115	1	4	81
104	13	3	1	9		232	29	3	1	9
106	53	1	1	3		234	117	1	9	19683
110	55	1	3	27		238	119	1	7	2187
112	7	4	1	17		240	15	4	3	4913
114	57	1	2	9		244	61	2	1	5
116	29	2	1	5		246	123	1	6	729
120	15	3	3	729		248	31	3	3	729
122	61	1	1	3		250	125	1	3	27
124	31	2	3	125		252	63	2	9	1953125
126	63	1	9	19683		254	127	1	9	19683
130	65	1	6	729		260	65	2	6	15625
136	17	3	2	81		266	133	1	7	2187
138	69	1	3	27		270	135	1	8	6561
140	35	2	4	625		272	17	4	2	289
142	71	1	1	3		274	137	1	2	9
146	73	1	4	81		276	69	2	3	125
148	37	2	1	5		280	35	3	4	6561
150	75	1	6	729		282	141	1	3	27
154	77	1	3	27		284	71	2	1	5
156	39	2	3	125		286	143	1	3	27

References

- [1] Castagnoli, G., Massey, J., Schoeller, P., Seeman, N., “On Repeated Root Cyclic Codes,” *IEEE Transactions on Information Theory*, pp. 337-342, March 1991.
- [2] Dicuangco, L.B., Moree P., Solé, P., “The Lengths of Hermitian Self-Dual Extended Duadic Codes,” *Journal of Pure and Applied Algebra* 209, pp. 223-237, 2007.
- [3] Dicuangco, L.B., Moree P., Solé, P., “On the Existence of Hermitian Self-Dual Extended Abelian Group Codes,” *Automorphic Forms, Springer Proceedings in Mathematics & Statistics*, Volume 115, pp 67-84, 2014.
- [4] Huffman, W.C., Pless, V., *Fundamentals of Error-Correcting Codes*, Cambridge University Press, New York, 2003.
- [5] Jia, Y., Ling, S., Xing, C., “On Self-Dual Cyclic Codes Over Finite Fields,” *IEEE Transactions on Information Theory*, pp. 2243-2251, April 2011.
- [6] Jitman, Y., Ling, S., Sole, P., “Hermitian Self-Dual Abelian Codes,” *IEEE Transactions on Information Theory*, pp. 1496-1507, March 2014.
- [7] Kai, X., Zhu, S., “On Cyclic Self-Dual Codes,” *AAECC*, vol. 19 pp. 509-525, 2008.
- [8] Ocampo, A., “On Euclidean Self-Dual Extended Split Group Codes,” Master’s Thesis, University of the Philippines, Diliman, 2010.
- [9] Nedeloaia, C., “Weight Distributions of Cyclic Self-Dual Codes,” *IEEE Transactions on Information Theory*, pp. 1582-1591, June 2003.
- [10] Sloane, N.J.A., Thompson, J.G. “Cyclic Self-Dual Codes” *IEEE Transactions on Information Theory*, pp. 364-366, May 1983.
- [11] Smid, Michiel H.M. “Duadic Codes,” *IEEE Transactions on Information Theory*, pp. 432-433, May 1987.
- [12] van Lint, J., “Repeated-Root Cyclic Codes,” *IEEE Transactions on Information Theory*, pp. 343-345, March 1991.
- [13] Zimmerman, K., “On Generalisations of Repeated-Root Cyclic Codes,” *IEEE Transactions on Information Theory*, pp. 641-649, March 1996.